CS4331/CS5342 Network Security
Homework 3

# Name: Venkata Nikhil Thanikella
# R#: R11904730

**Q.1. How many ways to achieve key distribution?**
**Ans:**

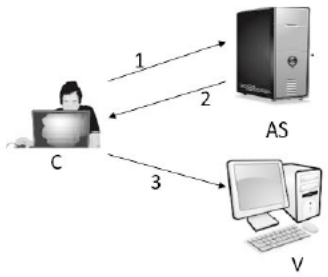
- A key could be selected by A and physically delivered to B.
- A third party could select the key and physically deliver it to A and B
- If A and B have previously and recently used a key, one party could transmit the new key to the other, using the old key to encrypt the new key.
- If A and Beach have an encrypted connection to a third-party C, C could deliver a key on the encrypted links to A and B

**Q.2. What are the requirements of many-to-many authentication?**
**Ans:**
**Security;** against attacks by eavesdroppers and malicious users
**Transparency:** users shouldn't notice authentication taking place.

- entering password is fine, if done rarely

**Scalability:** Large number of users and servers

**Q.3. What are advantages & weaknesses of this protocol?**



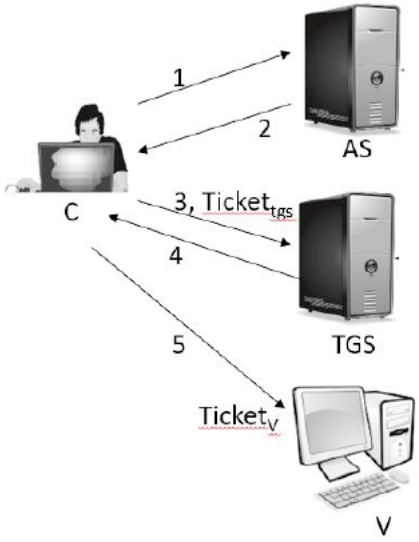

**Ans:**
1.C->AS: IDC||PC||10V
2. AS->C: Ticket E(KV) [IDC||ADC [LOV])
3. CV: IDC || Ticket

**Advantage**

- Client and malicious attacker cannot alter IDC (impersonate), ADC (change of address), IDV
- server V can verify the user is authenticated through IDC, and grants service to C
- guarantee the ticket is valid only if it is transmitted from the same client that initially requested the ticket.

**Weakness:** Insecure password is transmitted openly and frequently
**Solution:** no password transmitted by involving ticket-granting server (TGS)

**Q.4. What are advantages & weaknesses of secure authentication?**




**Ans:**
Once per user logon session

(1) CAS: IDC1OTgS
(2) ASCE(KC, Tickettgs)

Once per type of service:

(3) C-TGS: IDC |||DV|| Tickettgs
(4) TGS-C: TicketV

Once per service session;
(5) CV: IDC || TicketV

Advantage:

- No password transmitted in plaintext.
- Tickets are reusable. Timestamp is added to prevent reuse of ticket by an attacker.

Weakness

- Ticket hijacking
    - Malicious users may steal the service ticket of another user on the same workstation and try to use it.
    - Network address verification does not help.
    - Servers must verify that the user who is presenting the ticket is the same user to whom the ticket was issued.

No server authentication

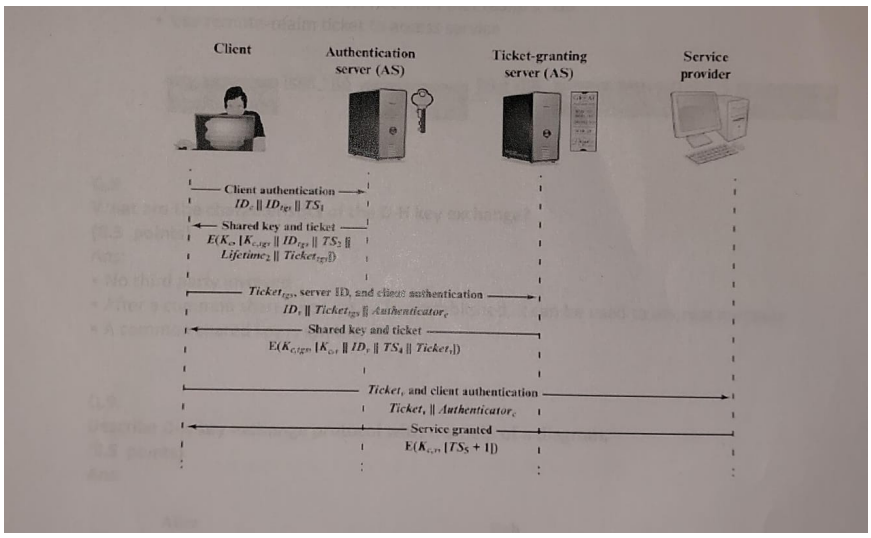
- Attacker may misconfigure the network so that he receives messages addressed to a legitimate server-man in the middle attack.

- Capture private information from users and/or deny service Servers must prove their identity to users.

- Servers must prove their identity to users.

Solution: section key

**Q.5.Draw & describe the sequence diagram of Kerberos_V4**
**Ans:**




**Q.6.What are the important ideas in Kerberos?**

**Ans**: Short-term session keys

- Long-term secrets used only to derive short-term keys • Separate session key for each user-server pair.

- Re-used by multiple sessions between same user and server-lifetime.

Proofs of identity based on authenticators.

- Client encrypts his identity, addr, time with session key; knowledge of key proves client has authenticated to KDC.
- • Also prevents replays (if clocks are globally synchronized)

• Server learns this key separately (via encrypted ticket that client can't decrypt), then verifies client's authenticator

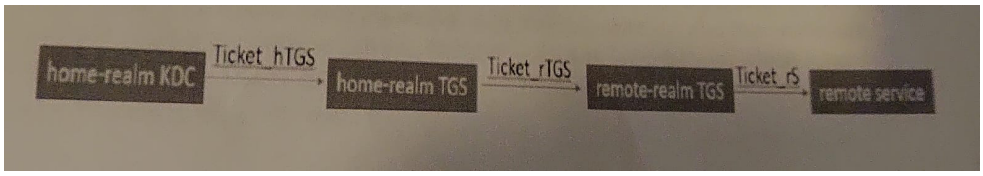
• Symmetric cryptography only

**7. Write a sequence to access the service in the remote realms to get the service ticket.**

**Ans:**

To access a service in another realm, users must...

- Get ticket for home-realm TGS from home-realm KDC.
- Get ticket for remote-realm TGS from home-realm TGS.
- As if remote-realm TGS were just another network service • Get ticket for remote service from that realm's TGS.
- Use remote-realm ticket to access service.




.

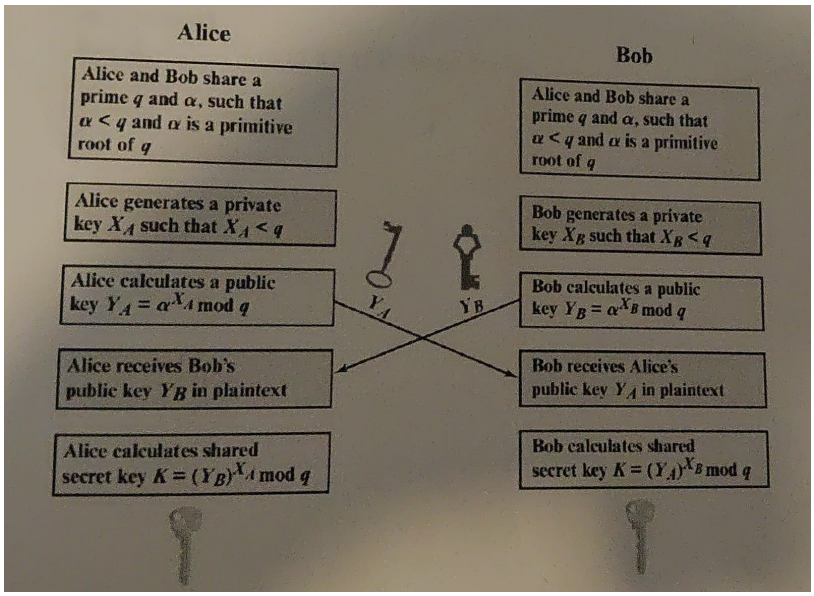
**Q.8. What are the characteristics of the D-H key exchange?**

**Ans:**

- No third party involved.
- After a common shared key, αX AXB is established, it can be used to encrypt messages.
- A common shared key is symmetric.

**Q.9.Describe D-H key exchange protocol with the help of a diagram.**

**Ans:**




**Q.10. What are the assumptions in D-H key exchange protocol?**

**Ans:** Two cryptographic assumptions: •

- Discrete logarithm problem (discrete log problem): Given a, q, $\alpha$^XA mod q for random XA, it is computationally hard to find XA.

• Diffie-Hellman assumption: Given a, q, $\alpha$ ^XA mod q, and $\alpha$^XB mod q for random X., Xв, no polynomial time attacker can distinguish between a random value R and QXAXB mod q.
• Intuition: The best-known algorithm is to first calculate XA and then compute

(QXB)XA mod q, but this requires solving the discrete log problem, which is hard! • Note: Multiplying the values doesn't work, since you get QXA+XB mod p$\neq$ QXAXB mod p

**Q.11.What attack is D-H key exchange suffer?**

**Ans:** David can alter messages, block messages, and send her own messages • DH is not secure against a MITM attacker: David can just do a DH with both sides!

**Q.12. Consider a Diffie-Hellman key exchange scheme with a common prime q = 11 and a primitive root $\alpha$ = 3. If User A has the public key $Y_A$ = 5, and User B has both the private key $Y_B$ = 4 and the private key $X_B$ = 4, what is the shared secret key K?**

**Ans:** K = (YA)^X8 mod q = (5) ^ 4 mode 11=9